Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 92 (2016) 461 – 467

Procedia Computer Science

2nd International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2016)

Srikanta Patnaik, Editor in Chief

Conference Organized by Interscience Institute of Management and Technology

Bhubaneswar, Odisha, India

Privacy Issues in Web Services: An Ontology based Solution

*Rekha Bhatia[a], Manpreet Singh[b]

[a]*Punjabi University Regional Centre, Mohali, India*

[b]Punjabi University, Patiala, India

Abstract

Privacy is the right of a person to specify that when, how and to what amount information about him is disclosed to others. Due to the tremendous use and popularity of web services, the likelihood of intentional and unintentional privacy disclosures is also increasing. The web services users generate a rich amount of information when they browse the websites of the service providers, access social networking sites to post their comments & product reviews, and store their data in the cloud. The data such generated is a voluminous and valuable treasure for the marketers as well as advertisers. The emerging technologies and fast increasing online activities of users are posing new threats to user's privacy and digital life. While accessing the web services, users unknowingly agree to the privacy policy of the service provider through which they authorize the service providers to collect and share their personally identifiable information. Most of the users think that while accepting the privacy policy of the service provider, they are protecting their privacy but actually they are signing the policy which informs them about the privacy rights they are surrendering to the service providers. In this paper, we aim to minimise the privacy related information disclosure of the user through various prevalent semantic web based technologies.

Peer-review under responsibility of the Organizing Committee of ICCC 2016

Keywords: Web Services; Privacy; Ontology; Privacy Disclosure; Privacy Parameters

Peer-review under responsibility of the Organizing Committee of ICCC 2016

doi:10.1016/j.procs.2016.07.368

1. Introduction

Due to the integration of web services in our daily life, abundance of privacy sensitive data about people is available in web based databases, which can be easily accessed by persons having malicious intentions. The basic reason behind this is the ease of web availability. The main idea about minimising privacy disclosure is to match the privacy policies of the service provider to the requirements of the service user so that privacy sensitive data of the service users is secured based on both the security policies as well as the privacy policies [1][2][3][4] [5].

This paper proposes a framework which solves client's privacy protection dilemma in the context of web services paradigm. The proposed framework and its practical applicability has been validated through an ontological implementation. The implementation model of our proposed framework uses the web ontology language OWL and semantic web rule language SWRL. We have undertaken a study about online shopping, in order to validate the authenticity of our framework. The organization of the paper is as follows: In the second section, related work in this area is discussed. In section 3, our proposed framework is described in detail. Finally, the paper is concluded with a mention of how automation of selecting the appropriate web service, can lead to the minimal undesired disclosure of user's sensitive personal data.

2. Related Work

The rise of the Semantic Web has given birth to a novel structure called ontology defined using Web Ontology Language (OWL) [6] which was used to provide interoperability [7][8][9]. Earlier work presented in [10] [11] [12] followed a similar approach like ours. The difference lies in that we have created ontology for storing privacy policies of the service providers incorporating a number of privacy related parameters.

3. Proposed Ontological Framework

First thing in any ontology is the description of its core concepts. Concepts are also known as classes and these classes are the core component of most of the ontologies. A Concept explains a group of different objects which share common characteristics. For example, humans share characteristics, such as a set of specific body parts, the ability to speak a language etc. Most of the ontology languages allow the developer to define classes on the basis of these characteristics. A class may be a subclass of another class; this means that if the classA is a subclass of B, then any individual of type A will also be an individual of type B. An individual represents objects in the real world e.g, RB_Company, IBM_Company etc. It is possible within ontology to explicitly state that A is a subclass of B; in some languages, including OWL it is also possible to infer this.Classes may also share associations with each other. These associations or relationships specify the way individuals of one class are associated with the individuals of another class.The Privacy ontology for online shopping scenario has four main classes: Web_Service_Entity, User_PII, Privacy_Policy, Permission. The Web_Service_Entity class has two sub classes named:Service_Provider and Service_User. Service providers specify their privacy policies in the Privacy_Policy class whereas service users specify their privacy preferences in the semantic web rule language based rules. The User_PII class contains personally identifiable information (PII) of service users:

1.Identification_Info: Identification information (name, address, passport number, PAN card number)
2. Contact_Info: Contact details (phone number, e-mail id)
3. Health_Info: Health information (disease, treatment, medicines)
4. Financial_Info: Financial information (bank account, locker number, property details)
5. Other_Info: Other privacy sensitive information (Any such information, which is regarded as sensitive by the user and which he wants to reveal selectively, will come under this class).

The Privacy_Policy class specifies the privacy policy of the service provider. It contains various parameters of privacy policies as specified below:

1. Granularity_Name: This parameter specifies whether PII name can be accessed at high, medium or low granularity level.
2. Granularity_Address: This parameter specifies whether PII address can be accessed at high, medium or low granularity level.
3. Purpose: This parameter states that for which purpose, like online survey or delivery of goods, the PII should be provided.
4. Trust: This parameter specifies the value of total trust in a service provider.
5. Consent: This parameter specifies whether the service provider is granted consent to access a particular piece of PII or not.
6. Retention-period: This parameter specifies, for how much time after providing the requested service, the PII of service user can be retained.
7. Access decision: This parameter specifies about the decision of the service provider after checking the privacy preferences of the service user.

The Permission class specify various actions which can be performed on user's personally identifiable information.

1. Permission_Collect: This permission specifies which piece of PII, the service provider is allowed to collect.
2. Permission_Share: This permission specifies whether the service provider is granted permission to share the service user's PII with third party collaborating service providers or not.
3. Permission_Access: This permission states that which service_provider is allowed to access the collected PII.
4. Permission_Publish: This permission specifies whether the collected PII of a service user can be made available online.

Table1: Some Object Properties and Possible Values

S.No.	Object_Property	Possible Values
1.	Access_Condition_is	a. Goods arrive in next 10 days b. Goods arrive in next 5 days c. Goods arrive in next 2 days
2.	Access_Purpose_is	a. Delivery of goods b. Providing service c. Marketing Survey
3.	Permission_Collect_Name_is	a. Granted b. Not Granted
4.	Retention_Period_is	a.Deleting privacy information immediately after providing service b. Retaining privacy information after providing service until next request
5.	Access_Decision_is	a. Agree to provide service b. Deny to provide service
6.	Granularity_Name_Is	a. High b. Medium c. Low
7.	Granularity_Address_Is	a. High b. Medium c. Low

Table 2: Domain and Range Restrictions for Object Properties

Object Property	Domain	Range	Description
Access_Condition_is	Service_Provider	Access_Condition	Service-Provider must fulfil the access condition
Access_Purpose_is	Service_Provider	Access_Purpose	For which purpose Service-Provider want to access the PII?

Permission_Collect_Name_is	Service_Provider	Access_Consent	Has Service-Provider been authorised for collecting PII name?
Retention_Period_is	Service_Provider	Retention_Period	For how much time the Service- Provider is authorized to retain PII?
Access_Decision_is	Service_Provider	Access_Decision	Whether Service-Provider will be able to provide service?
Granularity_Name_Is	Service_Provider	Granularity_Name	How much granularity for PII name is allowed?

Relationships in ontology are represented by two types of properties i.e. object properties and data properties. Object properties represent relationships between two individuals, e.g. hasSister, hasParent, worksFor etc. Data properties link individuals to concrete values, e.g., hasAge, hasValue, hasTrust etc. The values assumed by various object properties in privacy ontology are summarized in the Table 1 and domain and range of object properties are specified in table 2. A number of service providers are registered with the ontology in Service_Provider class along with their corresponding privacy policies in Privacy_Policy class through object property and data property concepts of ontology. An example of a privacy policy of a service provider is:

"The service provider requires access to the name, address and phone-number of the user in order to deliver goods ordered online. The service provider deletes details of the user PII immediately after providing service. The service provider is able to deliver goods within five days. The trust value of the service provider is 0.9."

Next, the privacy preferences of a user's access request are formulated into an SWRL rule and reasoned through an inference engine with the privacy policies of the service providers in order to find out the suitable service provider.

An SWRL rule is composed of an antecedent and a consequent. There are several forms for fragments of an SWRL rules, for example, Desc (a), Prop (p, q) etc. where Desc is an OWLdescription and Prop is an OWL property and a, p and q are either one of the three constituents i.e. OWL Variables, OWL Individuals and OWL Property/data values. An example SWRL rule specifying user privacy preferences is:

Service_Provider(?x) ∧ Permission_Collect_Name_Is(?x, Granted) ∧
Permission_Collect_Address_Is(?x, Granted) ∧ Permission_Collect_Phone_Is(?x, Granted) ∧
Access_Purpose_Is(?x, Delivery) ∧ Granularity_Name_Is(?x, High) ∧
Granularity_Address_Is(?x, high) ∧
Retention_Period_Is(?x, Deleting_Privacy_Information_Immediately_After_service) ∧
Access_Condition_Is(?x, Goods_Arrive_In_Next_2Days) ∧ Trust_Value(?x, 0.8)
→ Access_Decision_Is(?x, Access_Decision_Agree_To_Provide_service)

This rule states that if x is a service provider then he is granted permission to access name, address and phone no. (PII) at high granularity levels for the purpose of delivering goods only if he can deliver goods in next 2 days, deletes PII immediately after delivering service and his trust value is equal to 0.8. Another example showing SQWRL rule for querying the privacy ontology using SQWRL query language is as shown below. This rule states that if x is a service provider and he is granted permission to access name, address and phone no. (PII) at high granularity levels for the purpose of delivering goods and if he can deliver goods in next 2 days& deletes PII immediately after delivering service plushis trust value is equal to 0.8, then name that service provider.

Service_Provider(?x) ∧ Permission_Collect_Name_Is(?x, Granted) ∧
Permission_Collect_Address_Is(?x, Granted) ∧ Permission_Collect_Phone_Is(?x, Granted) ∧
Access_Purpose_Is(?x, Delivery) ∧ Granularity_Name_Is(?x, High) ∧
Granularity_Address_Is(?x, high) ∧
Retention_Period_Is(?x, Deleting_Privacy_Information_Immediately_After_service) ∧
Access_Condition_Is(?x, Goods_Arrive_In_Next_2Days) ∧ Trust_Value(?x, 0.8) ∧
Access_Decision_Is(?x, Access_Decision_Agree_To_Provide_service) →
sqwrl:select (?x)

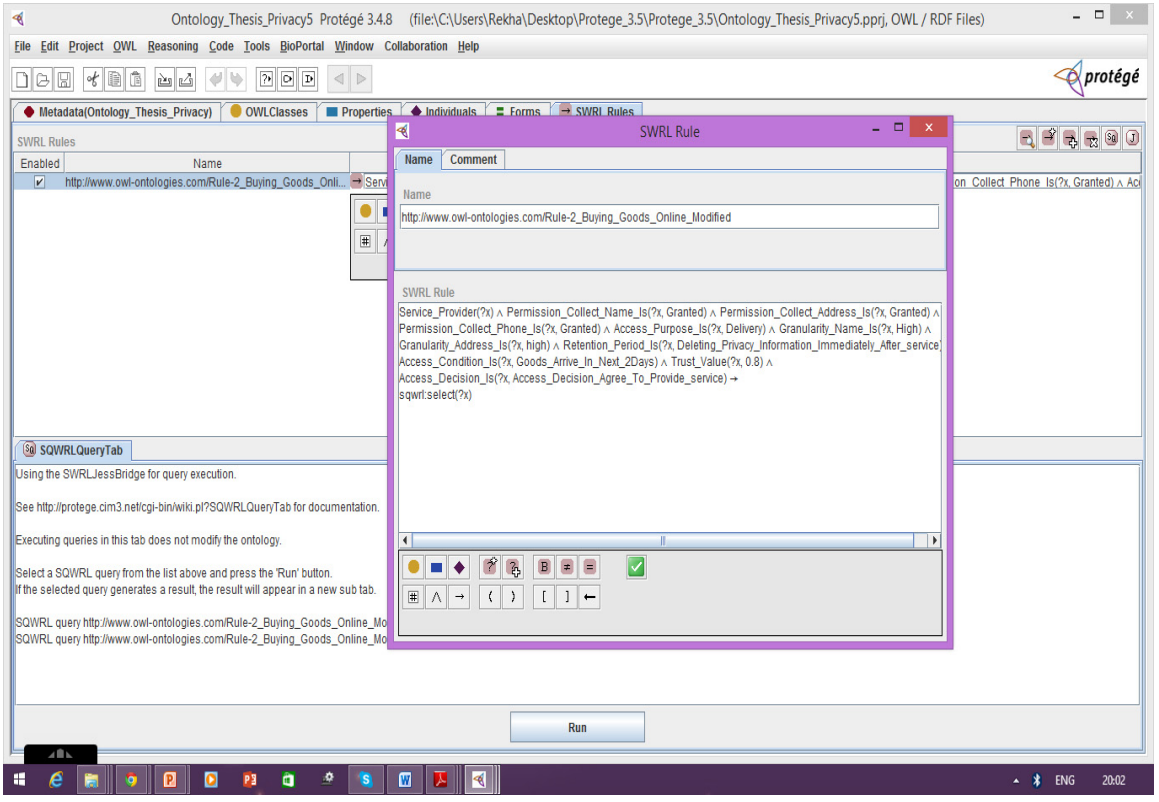

Fig 1: SQWRL Query in Privacy Ontology

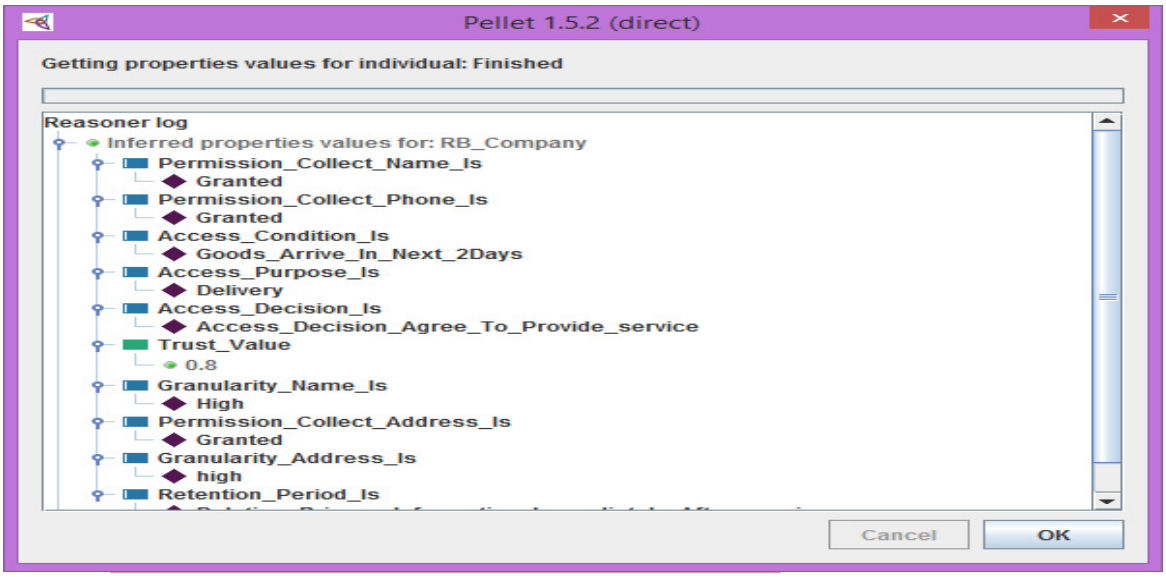

Fig 2: Inferred properties values through reasoner Pellet

We have compared the query response time of our model with the traditional access control model in which no privacy related information is present in the query. The result of this comparison is presented in figure 3. As expected, the inference time of our proposed model is a little bit more as compared to traditional access control model. This is justifiable as the inference time is dependent on the complexity of the policy. Moreover, the trend in the graph is linear which justifies the overhead of our approach in order to incorporate privacy in access control process of web services.

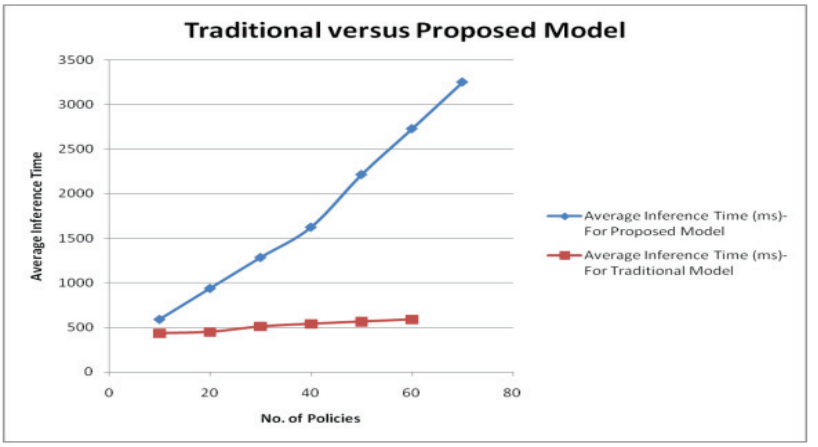

Fig 3: Traditional versus Proposed Solution

5. Conclusions

We have examined the performance of the developed framework and concluded that the time for making privacy aware access control decision through ontological implementation model is acceptable, as it imposes a small, acceptable overhead with the added advantage of minimal disclosure of sensitive personal data. By reasoning the SWRL rule based privacy preferences of the requesting user with the privacy domain ontology, we can select the desired web service provider from a host of service providers and protect the user privacy efficiently as well as effectively.

6. References

[1] C. A. Ardagna, M. Cremonini, S. De Capitani Di Vimercati, and P. Samarati, "A privacy-aware access control system," Journal of Computer Security, vol. 16, 2008, pp 369-397.
[2] M. Casassa Mont, R. Thyne, K. Chan, P. Bramhall (2005) http://www.hpl.hp.com/techreports/2005/HPL-005-110.pdf.
[3] H. Oberholzer and M. S. Olivier, Privacy contracts as an extension of privacy policies. International Conference on Data Engineering Workshops (ICDEW'05), 0:1192, 2005.
[4] J.W. Byun, E. Bertino, and N. Li, Purpose based access control for privacy protection in relational database systems. Technical Report 2004-52, Purdue University, 2004.
[5] R. Bhatia and M.S Gujral, An Implementation Model for Privacy Aware Access Control in Web Services Environment. Proceedings of International Conference on ICT for Sustainable Development (ICT4SD 2015), 2015.
[6] The World Wide Web Consortium (W3C): OWL Web Ontology Language Overview (February 2004).
[7] Mitra, P., Pan, C.C., Liu, P., Atluri, V.: Privacy-preserving semantic interoperation and access control of heterogeneous databases. In: ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security. pp. 66-77. ACM (2006)
[8] Pan, C.C., Mitra, P., Liu, P.: Semantic access control for information interoperation. In: SACMAT '06: Proceedings of the 11th ACM symposium on Access control models and technologies. pp. 237-246. ACM, New York, NY, USA (2006)

[9] Sun, Y., Pan, P., Leung, H.f., Shi, B.: Ontology based hybrid access control for automatic interoperation. In: Xiao, B., Yang, L., Ma, J., Muller-Schloer, C., Hua, Y. Autonomic and Trusted Computing, LNCS, vol. 4610, pp. 323-332. Springer Berlin / Heidelberg (2007)
[10] Garcia D, Toledo MBF, Capretz M, Allison D, "Towards a base ontology for privacy protection in service-oriented architecture", 2009 IEEE International Conference on Service-Oriented Computing and Applications (SOCA), pp. 1-8, 2009.
[11] Ge, Qiang, et al. "The Application of SWRL Based Ontology Inference for Privacy Protection." Journal of Software 9.5 : pp.1217-1222, 2014.
[12] Kayes, A. S. M., Han, J., & Colman, A. (2014, January). PO-SAAC: A Purpose-Oriented Situation-Aware Access Control Framework for Software Services. In Advanced Information Systems Engineering (pp. 58-74).Springer International Publishing.